4/PRTS

09/581459

[10191/1452]

SYSTEM FOR CONTROLLING ACCESS AUTHORIZATION

Background Information

The present invention is based on a system for controlling access authorization. ~~as set forth by~~ German Patent No. 44 28 947 has ~~the species defined in the independent claim. The German patent 44 28 947 C1 has~~ already described a locking device for a motor vehicle having an actuating device as well as a transponder. Upon actuation of a transmitter, a remote-actuation changeable code word can be generated; a decoding device receives the code word, compares it to a remote-actuation changeable code signal stored in the decoding device, and generates an unlocking signal as a function of the comparison. Moreover, to increase security, a transponder is provided whose changeable code signal is also evaluated for an enablement.

Summary Of the Invention

The object of the present invention is to simplify the aforesaid system without suffering a loss in security. ~~The objective is achieved by the characterizing features of the independent claim.~~

The system of the present invention for controlling access authorization includes a base device which receives a code word. The code word contains a response which a computer compares to a required response. An access is authorized if the response and the required response agree. At least one remote control transmits the code word. The system according to the present invention has the distinction that a challenge transmitted by the base device is stored in the remote control for generating the code word. This challenge is identical to that of a challenge/response process already successfully implemented in the past. Thus, the challenge gives an indication of an authorization of the remote control. In this manner, possibilities for manipulation are restricted. On the other hand, a fresh bidirectional challenge/response process is no longer necessary for the start of an access authorization procedure, since the challenge is already stored in the memory of the remote control. In this way, the code word can already be

EL302699756

transmitted with a greater transmission range to the base device, while the challenge/response procedure can only be carried out at short distance. Thus, a decoupling between bidirectional data transmission and unidirectional data transmission is ensured. Only a transmitter of greater transmission range is to be provided in the remote control, but not a corresponding receiver for the remote area. The challenge can be used for synchronization between the base device and remote control. In addition, the response and the required response, respectively, directly decisive for the access authorization are not stored in either the base device or in the remote control, so that direct access to this security-relevant information is not possible.

In an expedient further development, the required response is formed as a function of an identifier stored in the remote control and contained in the code word. In this manner, an unequivocal allocation is achieved between the remote control used and the corresponding encryption stored in the base device. A clear allocation guarantees sufficiently high security against unauthorized manipulation attempts. Because of this, the algorithm which, in the remote control, encrypts the stored challenge - for example, using an identifier specific to the remote control - to form a response can simply be omitted and integrated in a microcontroller.

In one refinement, the challenge stored in the base device is erased after a predefined number of failed agreements of response and required response. This ensures that, given a number of failed opening attempts, an access is no longer authorized in response to further attempts. A renewed opening attempt is only to be permitted in conjunction with a successfully flowing challenge/response process. Upon failure of the access authorization via the unidirectional protocol, the security requirements are increased, in that an access can only be achieved in conjunction with the complex bidirectional protocol.

According to one advantageous refinement, the code word includes a counter code which the base device compares to a reference code. An access is only authorized in response to a deviation. The counter code is changed with the actuation of an operating control element of the remote control. Transmission of the code word just monitored does not trigger an access authorization. The counter reading can be present both in unencrypted and in encrypted form in the code word.

A transmitted code is used as reference code. A separate counter function does not have to be provided in the base device for this purpose.

Expediently, the code word is transmitted at high frequency and the challenge is transmitted at low frequency. Because of the stored challenge, the remote control does not need a receiver in the high-frequency range.

~~Other useful further developments come to light from the description and from further~~ dependent claims.

Drawing

InsA

Two possible exemplary embodiments of a system according to the present invention for controlling access authorization are shown in the drawing and are explained in greater detail in the following description. Figures 1 and 2 show a block diagram and an access authorization procedure of a first exemplary embodiment; Figures 3 and 4 show a block diagram and an access authorization procedure of a second exemplary embodiment.

~~Description~~

A plurality of remote controls F1, ... Fx, ... Fn communicate with a base device BG which includes a transmitter/receiver 12 and a computer 16. Computer 16 exchanges data with transmitter/receiver 12 and has access to challenges C1, ... Cx, ... Cn, identifiers K1, ... Kx, ... Kn and a limiting value G stored in the memory. The design of the xth remote control Fx is shown by way of example. A remote-control computer 20 has access to identifier Kx and challenge Cx stored in the memory. It supplies data to transmitter 22 and exchanges data with a remote-control transmitter/receiver 26. The signal state influenced by an operating control element 24 is supplied to remote-control computer 20.

The second exemplary embodiment according to Figure 3 differs from the first exemplary embodiment according to Figure 1 in that, instead of limiting value G, a memory for a reference code RZ1, ... RZx, ... RZn is provided in base device BG. Remote control Fx has an additional field for a counter code Zx.

In the following, the functioning method of the first exemplary embodiment shown in Figure 1 is explained in greater detail. A corresponding identifier K1, ... Kx, ... Kn is stored in base device BG for each remote control F1, ... Fx, ... Fn. Because of this, base device BG is able to clearly identify each individual remote control Fx or each remote-control group Fx - if, for example, a plurality of remote controls Fx are allocated to one identifier Kx. These identifiers K1, ... Kx, ... Kn can be the corresponding memory locations, i.e., can be recognized on the basis of the memory location. In the challenge/response process, the base device transmits challenge Cx to remote control Fx clearly allocated by identifier Kx. A random-sequence generator generates this challenge Cx. Computer 16 stores transmitted challenge Cx in a memory location addressed via identifier Kx. Remote-control computer 20 stores the challenge Cx last transmitted by base device BG in a memory.

The user starts the unidirectional communication of remote control Fx with base device BG by actuating operating control element 24, step 101. Using information specific for the special remote control Fx, remote-control computer 20 combines challenge Cx, stored in the memory, with an algorithm, from which response Rx is formed. For example, a part of identifier Kx, a manufacturing code permanently stored in remote control Fx, is used as information specific to the remote control. However, ~~it is essential that~~ this encryption, i.e., algorithm and information specific to the remote control, of challenge Cx is ~~be~~ known and stored for each remote control Fx in base device BG, as well. Code word CWx contains identifier Kx and response Rx and, if desired, appropriate wake-up and action commands. Transmitter 22 sends code word CWx to base device BG, step 103. Computer 16 filters identifier Kx out from received code word CWx. Computer 16 selects the challenge Cx, addressed by this identifier Fx, and encryption, which were also used to ascertain response Rx in remote control Fx. Computer 16 calculates required response Sx from challenge Cx, stored in base device BG, from the algorithm and from the information specific to the remote control, thus from the encryption, step 105. Received response Rx and calculated required response Sx are compared in base device BG, step 107. If they agree, computer 16 gives a corresponding enabling signal, step 109. Otherwise, query 111, as to whether the number of failed opening attempts M has already exceeded a specifiable limiting value G, follows. If this is the case, no further opening attempt is permitted, step 113. In addition, challenge Cx stored in base device BG is erased. Thus, an access authorization can only be achieved by a successful run-through of the bidirectional challenge/response procedure, but not with the unidirectional protocol described. If the number of failed opening attempts M has not yet exceeded limiting value G, number M is incremented, step 115. Following this is step 105; the further procedure takes its course as already described.

The steps from 111 on increase the security of the unidirectional data transmission, but are not absolutely necessary.

The second exemplary embodiment, described in the following, relates to Figures 3 and 4. As already explained for the first exemplary embodiment, challenge Cx is stored in remote control Fx. A counter code Zx, which is incremented in response to actuation of the operating control element 24, is stored in remote control Fx. For each remote control Fx, the last transmitted counter code Zx is stored as reference code RZ1, ... RZx, ... RZn in base device BG. After the start has been triggered by actuating operating control element 24, step 121, in conformity with the first exemplary embodiment, response Rx is calculated. Counter code Zx is increased by one. In addition to response Rx and identifier Kx, counter code Zx is contained in encrypted form in code word CWx. Transmitter 22 sends code word CWx to transmitter/receiver 12, step 123. Computer 16 in turn filters identifier Kx out from received code word CWx, and reads out reference code RZx belonging to remote control Fx on the basis of this identifier, step 125. Counter code Zx is subsequently compared to reference code RZx, step 127. Since the counter code Zx last transmitted is stored as reference code RZx in base device BG, given a proper actuation of remote control Fx, counter code Zx and reference code RZx deviate from one another. However, if they agree, the procedure is broken off, step 129. An access is not authorized. Otherwise, as already for the first exemplary embodiment, base device BG ascertains required response Sx, step 131. If response Rx and required response Sx do not agree, step 133, then the procedure is broken off, step 135. Otherwise the authorization is given for initiating an opening operation, step 137.

As an alternative second exemplary embodiment, counter code Zx is encrypted in remote control Fx. To ascertain reference code RZx, this encryption is ~~must be~~ stored, addressed, in base device BG. It is only important for counter code Zx that it change with each actuation of remote control Fx; whether by a counter function or another algorithm is not important.

The two exemplary embodiments can also be combined to the effect that, for example, in the sequence according to Figure 4, the query according to step 111 is carried out. In this manner, security can be further increased vis-à-vis unauthorized opening attempts.

The challenge/response procedure, not explained more precisely, is preferably carried out at low frequency at short distance of the space to be entered, e.g., a motor vehicle. On the other hand, transmitter 22 transmits a higher-frequency signal which permits a greater transmission range. A receiver in the higher-frequency range is not to be provided for remote control Fx. The algorithm for encrypting challenge Cx in order to obtain response Rx can preferably be realized so simply that it too can be implemented in a microcontroller.